On Skolemising Zermelo's Set Theory

Alexandre Miquel

ON SKOLEMISING ZERMELO'S SET THEORY

ALEXANDRE MIQUEL

Abstract. We give a Skolemised presentation of Zermelo's set theory (with notations for comprehension, powerset, etc.) and show that this presentation is conservative w.r.t. the usual one (where sets are introduced by existential axioms). Conservativity is achieved by an explicit deskolemisation procedure that transforms terms and formulæ of the extended language into provably equivalent formulæ of the core language of set theory.

Finally we show that the notation $\{t(x) \mid x \in u\}$ ('the set of all $t(x)$ where x ranges over u') is also definable in this framework, which proves that the weak form of replacement which is needed to define syntactic constructs such as (set-theoretic) λ-abstraction and infinitary Cartesian product does not need Fraenkel and Skolem's replacement scheme to be justified.

§1. Introduction. Set theory [2, 3] is traditionally presented with a very economical first-order language whose atomic formulæ are built from two binary predicate symbols $=$ and $\in$ and whose underlying term algebra is reduced to variables—the language provides no constant or function symbol.

Although convenient in the perspective of a model-theoretic study, the language of set theory is too rudimentary to be used to formalise mathematics effectively. For a practical use, it is necessary to enrich the language of terms with notations to represent sets and set formers—and then to justify the conservativity of adding such notations. Justifying the conservativity of new notations is easy when these notations simply consist of Skolem symbols [5, 4]—typically, the function symbols $\{\_;\_\}$, $\mathfrak{P}(\_)$ and $\bigcup\_$ that are obtained by Skolemising pairing, powerset and union—since the introduction of Skolem function symbols is known to be conservative (both in classical and intuitionistic logic). The problem arises with the notation for comprehension

$$\{x \in t \mid \phi\}$$

(where t is a term and ϕ a formula depending on x) that does not only go beyond Skolem's conservativity result, but that also escapes the scope of first-order theories, where individuals are represented by first-order terms only.

To solve this problem for Zermelo's set theory [2, 3], Dowek introduces [1] Skolem symbols $\{\_;\_\}$, $\mathfrak{P}(\_)$, $\bigcup\_$ and ω for pairing, powerset, union and infinity, as well as, for every formula $\phi_{x_1,\dots,x_n,x}$ of the core language of set theory whose free variables occur among the variables $x_1,\dots,x_n$ and x, a Skolem symbol $f_{\phi_{x_1,\dots,x_n,x}}$ of arity $n+1$ such that $f_{\phi_{x_1,\dots,x_n,x}}(x_1,\dots,x_n,a)$ denotes the set of all $x \in a$ such that $\phi_{x_1,\dots,x_n,x}$. From these symbols, the notation $\{x \in a \mid \phi\}$ is then redefined for arbitrary formulæ ϕ using an encoding technique similar to λ-lifting. The main advantage of this approach is that despite its higher-order taste, the language of terms is still first-order since the notation $\{x \in a \mid \phi\}$ is but a macro which internally refers to a complex term built from a well-chosen set of Skolem symbols. However, the full justification of this approach ultimately relies on Skolem's theorem, whose complex and non constructive proof (based on the completeness theorem) gives no hint on how the removal of all these notations (a.k.a. deskolemisation) could be achieved effectively.

In this paper we give a direct justification of these notations for Zermelo's set theory by presenting an effective deskolemisation procedure that transforms every formula of the enriched language into a formula of the core language of set theory which is provably equivalent. The main ingredient of the translation is that every term t of the extended language is represented in the core language of set theory not as a characterising predicate ('x is t'), but as a predicate written $x \in^* t$ that characterises t as the collection of its elements (following the spirit or realisability). Using this method we get an elementary and fully constructive proof of conservativity of the extended theory—written Z^{sk}—far from the complexity of Skolem's theorem.

Of course, the primary interest of Z^{sk} is that its term language can express most standard mathematical notations—for the empty set, binary intersections and unions, ordered pairs, function application, Cartesian products, etc.—simply as macros. Surprisingly, it turns out that this term language is even rich enough to express the syntactic construct

$$\{t(x) \mid x \in u\}$$

which is traditionally justified using Fraenkel-Skolem's replacement scheme.[1] Technically, the definability of this notation comes from the fact that from two arbitrary terms $t(x)$ and u of Z^{sk} one can effectively extract a syntactic upper bound $\mathsf{B}\,(t(x) \mid x \in u)$ of the set of all $t(x)$ where x ranges over u, that is, a term $\mathsf{B}\,(t(x) \mid x \in u)$ such that the formula

$$\forall x\ (x \in u \ \Rightarrow\ t(x) \in \mathsf{B}\,(t(x) \mid x \in u))$$

is provable in the enriched system. Once the notation $\{t(x) \mid x \in u\}$ has been defined (as a subset of $\mathsf{B}\,(t(x) \mid x \in u)$ by comprehension), it is easy to derive notations for well-known binders such as

$$\lambda x \in A\,.\,t(x)\,, \qquad \bigcup_{x\in A} B(x)\,, \qquad \sum_{x\in A} B(x)\,, \qquad \text{etc.}$$

which shows that these syntactic constructs—traditionally justified using the replacement scheme—are actually definable inside Zermelo's axiomatics.

Outline of the paper. In Section 2 we recall the language of set theory and the axioms of Zermelo's set theory. In Section 3 we introduce a formal system called Z^{sk} (the skolemised presentation of Zermelo's set theory) and show how terms and formulæ of Z^{sk} can be transformed into formulæ of set theory that are provably equivalent. We study the properties of these transformations, from which we deduce that Z^{sk} is a conservative extension of Z. Finally, we show in Section 4 how most standard mathematical abbreviations can be defined in

[1]Formally, this means that all the instances of the replacement scheme that correspond to functional relations of the form $y = t(x)$ where $t(x)$ is expressed in the term language of Z^{sk} are provable in Zermelo's system.

the term language of Z^{sk} as macros. We also give a syntactic definition of the notation $\{t(x) \mid x \in u\}$ without using the replacement scheme.

§2. Zermelo's set theory.

2.1. The language of set theory. The core language of set theory is the language of (mono-sorted) first-order predicate logic whose atomic formulæ are built from two binary relations $x = y$ (*equality*) and $x \in y$ (*membership*):

Formulæ
$$\begin{array}{rcl} \phi, \psi & ::= & x = y \ \mid \ x \in y \ \mid \ \top \ \mid \ \bot \\ & \mid & \phi \wedge \psi \ \mid \ \phi \vee \psi \ \mid \ \phi \Rightarrow \psi \\ & \mid & \forall x\ \phi \ \mid \ \exists x\ \phi \end{array}$$

Note that this language provides no constant or function symbol, hence the term algebra is reduced to variables. In what follows, we shall use the following standard shorthands

$$\begin{array}{rclrcl} \neg\phi & \equiv & \phi \Rightarrow \bot & \phi \Leftrightarrow \psi & \equiv & (\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi) \\ x \neq y & \equiv & \neg(x = y) & x \notin y & \equiv & \neg(x \in y) \\ \forall x \in a\ \phi & \equiv & \forall x\ (x \in a \Rightarrow \phi) & \exists x \in a\ \phi & \equiv & \exists x\ (x \in a \wedge \phi) \end{array}$$
$$\begin{array}{rcl} \exists! x\ \phi & \equiv & \exists x\ (\phi\ \wedge\ \forall y\ (\phi\{x := y\} \Rightarrow y = x)) \\ x \subseteq y & \equiv & \forall z\ (z \in x\ \Rightarrow\ z \in y) \end{array}$$

as well as the macro $\mathrm{nat}(n)$ expressing that n is a finite ordinal:

$$\begin{array}{rcll} \mathrm{nat}(n) & \equiv & \forall x \in n\ x \notin x & \wedge \\ & & \forall x \in n\ \forall y \in x\ y \in n & \wedge \\ & & \forall x \in n\ \forall y \in x\ \forall z \in y\ z \in x & \wedge \\ & & \forall p\ (p \subseteq n \wedge \exists x\,(x \in p)\ \Rightarrow\ \exists x \in p\ \forall y \in p\ (x \in y \vee x = y)) & \wedge \\ & & \forall p\ (p \subseteq n \wedge \exists x\,(x \in p)\ \Rightarrow\ \exists x \in p\ \forall y \in p\ (y \in x \vee y = x)) & \end{array}$$

2.2. Axioms and deduction rules. As a first-order theory with equality, Zermelo's set theory comes with equality axioms expressing that equality is an equivalence relation

(Reflexivity)	$\forall x\ (x = x)$
(Symmetry)	$\forall x\ \forall y\ (x = y \Rightarrow y = x)$
(Transitivity)	$\forall x\ \forall y\ \forall z\ (x = y \wedge y = z \Rightarrow x = z)$

and that membership is compatible with equality

(Compat-Left)	$\forall x\ \forall x'\ \forall y\ (x = x' \wedge x \in y \Rightarrow x' \in y)$
(Compat-Right)	$\forall x\ \forall y\ \forall y'\ (y = y' \wedge x \in y \Rightarrow x \in y')$

From these axioms one easily derives Leibniz principle:

Proposition 1 (Leibniz principle). — *For every formula ϕ of the core language of set theory and for all variables x, x_1, x_2, the formula*

$$x_1 = x_2\ \Rightarrow\ (\phi\{x := x_1\} \Leftrightarrow \phi\{x := x_2\})$$

is intuitionistically derivable from the 5 equality axioms given above.

Proof. By induction on ϕ using equality axioms for atomic formulæ. ⊣

The remaining axioms of the theory—a.k.a. Zermelo's axioms—are the extensionality axiom, plus five existential axioms that express how sets can be constructed in the theory:

(Extensionality)	$\forall x\, \forall y\, (\forall z\, (z \in x \Leftrightarrow z \in y) \;\Rightarrow\; x = y)$
(Pairing)	$\forall x_1\, \forall x_2\, \exists y\, \forall z\, (z \in y \;\Leftrightarrow\; z = x_1 \vee z = x_2)$
(Comprehension)	$\forall x_1 \cdots \forall x_n\, \forall x\, \exists y\, \forall z\, (z \in y \;\Leftrightarrow\; z \in x \wedge \phi)$
(Powerset)	$\forall x\, \exists y\, \forall z\, (z \in y \;\Leftrightarrow\; z \subseteq x)$
(Union)	$\forall x\, \exists y\, \forall z\, (z \in y \;\Leftrightarrow\; \exists u\, (u \in x \wedge z \in u))$
(Infinity)	$\exists y\, \forall z\, (z \in y \;\Leftrightarrow\; \mathrm{nat}(z))$

(where comprehension axioms are introduced for every formula ϕ with free variables $x_1, \ldots, x_n, x, z$).

Zermelo's set theory (Z) is then defined as the classical first-order theory whose language is the (core) language of set theory and whose axioms are the equality axioms and Zermelo's axioms. *Intuitionistic Zermelo's set theory* (IZ) is the theory formed on the same language and the same system of axioms, but in which all reasoning is done in intuitionistic logic.

In this paper, we assume that proofs are done in natural deduction based on asymmetric sequents of the form $\Gamma \vdash \phi$, where Γ is a finite list of formulæ and ϕ a formula. The deduction rules are recalled in Fig. 1; they comprise all the rules of intuitionistic natural deduction, plus a rule which implements *reductio ad absurdum* to recover the full strength of classical logic.

A closed formula ϕ is a *theorem* of Z (resp. of IZ) when $\Gamma \vdash \phi$ is classically (resp. intuitionistically) derivable for some finite list of axioms Γ.

(Ax.)
$$\frac{}{\Gamma \vdash \phi}\ \phi \in \Gamma$$

$(\top,\ \bot)$
$$\frac{}{\Gamma \vdash \top} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}$$

$(\wedge)$
$$\frac{\Gamma \vdash \phi_1 \quad \Gamma \vdash \phi_2}{\Gamma \vdash \phi_1 \wedge \phi_2} \qquad \frac{\Gamma \vdash \phi_1 \wedge \phi_2}{\Gamma \vdash \phi_1} \quad \frac{\Gamma \vdash \phi_1 \wedge \phi_2}{\Gamma \vdash \phi_2}$$

$(\vee)$
$$\frac{\Gamma \vdash \phi_1}{\Gamma \vdash \phi_1 \vee \phi_1} \quad \frac{\Gamma \vdash \phi_2}{\Gamma \vdash \phi_1 \vee \phi_2} \qquad \frac{\Gamma \vdash \phi_1 \vee \phi_2 \quad \Gamma, \phi_1 \vdash \psi \quad \Gamma, \phi_2 \vdash \psi}{\Gamma \vdash \psi}$$

$(\Rightarrow)$
$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi} \qquad \frac{\Gamma \vdash \phi \Rightarrow \psi \quad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

$(\forall)$
$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \forall x\, \phi}\ x \notin FV(\Gamma) \qquad \frac{\Gamma \vdash \forall x\, \phi}{\Gamma \vdash \phi\{x := t\}}$$

$(\exists)$
$$\frac{\Gamma \vdash \phi\{x := t\}}{\Gamma \vdash \exists x\, \phi} \qquad \frac{\Gamma \vdash \exists x\, \phi \quad \Gamma, \phi \vdash \psi}{\Gamma \vdash \psi}\ x \notin FV(\Gamma, \psi)$$

(Abs.)
$$\frac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \phi}$$

Figure 1. Rules of natural deduction (including *reductio ad absurdum*)

§3. A Skolemised presentation of set theory. In this section, we introduce a formal system Z^{sk} that extends Zermelo's set theory with notations to express sets defined using Zermelo's existential axioms, and show that this formal system is a conservative extension of Zermelo's set theory (both in intuitionistic and classical logic).

3.1. The language of Z^{sk}. The language of Z^{sk} is built by enriching the term language of set theory with notations to express unordered pairs, powersets, sets defined by comprehension, etc. Formulæ are defined using the same syntactic constructs as usual, but since terms may now refer to formulæ, both syntactic categories of terms and formulæ need to be defined by mutual induction:

Terms $$\begin{array}{rcl} t, u & ::= & x \ \mid \ \omega \\ & \mid & \{t_1; t_2\} \ \mid \ \mathfrak{P}(t) \ \mid \ \bigcup t \\ & \mid & \{x \in t \mid \phi\} \end{array}$$

Formulæ $$\begin{array}{rcl} \phi, \psi & ::= & t = u \ \mid \ t \in u \ \mid \ \top \ \mid \ \bot \\ & \mid & \phi \wedge \psi \ \mid \ \phi \vee \psi \ \mid \ \phi \Rightarrow \psi \\ & \mid & \forall x\ \phi \ \mid \ \exists x\ \phi \end{array}$$

Free and bound occurrences of variables are defined as expected (both in terms and formulæ), keeping in mind that the notation $\{x \in t \mid \phi\}$ binds all the free occurrences of the variable x in the formula ϕ, but none of the free occurrences of the variable x in the term t (that refer to the enclosing context). The set of *free variables* of a term t (resp. of a formula ϕ) is written $FV(t)$ (resp. $FV(\phi)$). In particular we have:

$$\begin{array}{rcl} FV(\forall x\, \phi) \ = \ FV(\exists x\, \phi) & = & FV(\phi) \setminus \{x\} \\ FV(\{x \in t \mid \phi\}) & = & FV(t) \cup (FV(\phi) \setminus \{x\}) \end{array}$$

As usual, terms and formulæ are considered up to α-conversion. Given a formula ϕ, a variable x and terms t and u, we write:

- $t\{x := u\}$ the term which is obtained by substituting the term u to every free occurrence of the variable x in the term t;
- $\phi\{x := u\}$ the formula which is obtained by substituting the term u to every free occurrence of the variable x in the formula ϕ.

Both forms of substitutions are defined as expected, taking care of renaming bound variables to prevent undesirable captures.

3.2. The axioms of Z^{sk}. The axioms of Z^{sk} are the equality axioms and the axiom of extensionality (the same as before), plus the following Skolemised versions of Zermelo's axioms:

(PAIRING$^{\mathrm{sk}}$)	$\forall x_1\ \forall x_2\ \forall z\ (z \in \{x_1; x_2\} \ \Leftrightarrow \ z = x_1 \vee z = x_2)$
(COMPR.$^{\mathrm{sk}}$)	$\forall x_1 \cdots \forall x_n\ \forall x\ \forall z\ (z \in \{y \in x \mid \phi\} \ \Leftrightarrow \ z \in x \wedge \phi\{y := z\})$
(POWERSET$^{\mathrm{sk}}$)	$\forall x\ \forall z\ (z \in \mathfrak{P}(x) \ \Leftrightarrow \ z \subseteq x)$
(UNION$^{\mathrm{sk}}$)	$\forall x\ \forall z\ (z \in \bigcup x \ \Leftrightarrow \ \exists y\ (y \in x \wedge z \in x))$
(INFINITY$^{\mathrm{sk}}$)	$\forall z\ (z \in \omega \ \Leftrightarrow \ \mathrm{nat}(z))$

(As in the usual presentation of Zermelo's theory, the comprehension scheme defines a comprehension axiom for every formula ϕ whose free variables occur among the variables $x_1, \ldots, x_n, x, z$.) The deduction rules are the same as before (see Fig. 1), except that sequents are now written using formulæ of the extended language. The intuitionistic fragment of Z^{sk} is written $\mathrm{IZ}^{\mathrm{sk}}$.

Notice that compatibility axioms of Z^{sk} only deal with the membership relation, as in Zermelo's set theory. Indeed, there is no need to add compatibility axioms for the new notations—even comprehension—since the compatibility property associated to a given notation can be easily (and intuitionistically) derived from the corresponding skolemised axiom using extensionality:[2]

Proposition 2 (Compatibility). — *The following formulæ*

$$\begin{array}{ll}
(1) & \forall x\ \forall x'\ \forall y\ (x = x' \ \Rightarrow\ \{x; y\} = \{x'; y\}) \\
(2) & \forall x\ \forall y\ \forall y'\ (y = y' \ \Rightarrow\ \{x; y\} = \{x; y'\}) \\
(3) & \forall x\ \forall x'\ (x = x' \ \Rightarrow\ \mathfrak{P}(x) = \mathfrak{P}(x')) \\
(4) & \forall x\ \forall x'\ (x = x' \ \Rightarrow\ \bigcup x = \bigcup x') \\
(5) & \forall x_1 \cdots \forall x_n\ \forall x\ \forall x'\ (x = x' \ \Rightarrow\ \{y \in x \mid \phi\} = \{y \in x' \mid \phi\}) \\
(6) & \forall x_1 \cdots \forall x_n\ \forall x\ (\forall y\ (\phi \Leftrightarrow \phi') \ \Rightarrow\ \{y \in x \mid \phi\} = \{y \in x \mid \phi'\})
\end{array}$$

(where ϕ and ϕ' are arbitrary formulæ whose free variables occur among the variables $x_1, \ldots, x_n$ and x) are theorems of $\mathrm{IZ}^{\mathrm{sk}}$.

Proof. (1) Assume that $x = x'$. Under this assumption, we can derive:

1. $\forall z\ (z = x \Leftrightarrow z = x')$, using symmetry and transitivity of equality;
2. $\forall z\ (z = x \lor z = y \Leftrightarrow z = x' \lor z = y)$ from 1, by purely logical means;
3. $\forall z\ (z \in \{x; y\} \Leftrightarrow z = x \lor z = y)$, by (Pair$^{\mathrm{sk}}$);
4. $\forall z\ (z \in \{x'; y\} \Leftrightarrow z = x' \lor z = y)$, by (Pair$^{\mathrm{sk}}$);
5. $\forall z\ (z \in \{x; y\} \Leftrightarrow z \in \{x'; y\})$, from 2, 3 and 4;
6. $\{x; y\} = \{x'; y\}$ from 5, by extensionality.

The proofs of (2), (3), (4) and (5) are analogous.

(6) Under the assumption $\forall y\ (\phi \Leftrightarrow \phi')$, we can derive:

1. $\forall z\ (z \in x \land \phi\{y := z\} \Leftrightarrow z \in x \land \phi'\{y := z\})$, by purely logical means;
2. $\forall z\ (z \in \{y \in x \mid \phi\} \Leftrightarrow z \in x \land \phi\{y := z\})$, by (Compr.$^{\mathrm{sk}}$);
3. $\forall z\ (z \in \{y \in x \mid \phi'\} \Leftrightarrow z \in x \land \phi'\{y := z\})$, by (Compr.$^{\mathrm{sk}}$);
4. $\forall z\ (z \in \{y \in x \mid \phi\} \Leftrightarrow z \in \{y \in x \mid \phi'\})$, from 1, 2 and 3.
5. $\{y \in x \mid \phi\} = \{y \in x \mid \phi'\}$ from 4, by extensionality.

$\dashv$

From Prop. 2 we can derive Leibniz principle for terms and formulæ:

Proposition 3 (Leibniz principle). — *For all terms t and for all formulæ ϕ of the language of* Z^{sk}*, the universal closures of the formulæ*

$$\begin{array}{lcl}
x_1 = x_2 & \Rightarrow & t\{x := x_1\} = t\{x := x_2\} \\
x_1 = x_2 & \Rightarrow & \phi\{x := x_1\} \Leftrightarrow \phi\{x := x_2\}
\end{array}$$

are theorems of $\mathrm{IZ}^{\mathrm{sk}}$.

Proof. By mutual induction on t and ϕ. $\dashv$

Of course, $(\mathrm{I})\mathrm{Z}^{\mathrm{sk}}$ is an extension of (I)Z:

[2] Notice that we need two compatibility properties for the notation for comprehension: one for the bounding set x (5) and another one for the selection formula ϕ (6).

PROPOSITION 4 (Extension). — *If* $(\mathrm{I})\mathrm{Z} \vdash \phi$, *then* $(\mathrm{I})\mathrm{Z}^{\mathrm{sk}} \vdash \phi$.

PROOF. We only have to check that every axiom of Zermelo's set theory is a theorem of $\mathrm{IZ}^{\mathrm{sk}}$, which is obvious. $\dashv$

3.3. The deskolemisation procedure. The deskolemisation procedure of the language Z^{sk} relies on two transformations:

- A transformation on terms, which maps every term t of Z^{sk} equipped with a variable z to a formula of set theory written $z \in^* t$;
- A transformation on formulæ, which maps every formula ϕ of Z^{sk} to a formula of set theory written ϕ^*.

Both transformations are defined by induction on the sizes of t and ϕ from the deskolemisation equations given in Fig. 2. In this figure, we assume that the bound variable names that are introduced in the r.h.s. of defining equations are fresh w.r.t. the corresponding l.h.s. (On the other hand, we do not assume anything about the variable z in the definition of $z \in^* t$, and z is allowed to be one of the free variables of t.)

$$\begin{array}{lcl}
z \in^* x & \equiv & z \in x \\
z \in^* \omega & \equiv & \mathrm{nat}(z) \\
z \in^* \{t_1; t_2\} & \equiv & (z = t_1)^* \ \vee \ (z = t_2)^* \\
z \in^* \mathfrak{P}(t) & \equiv & \forall x \ (x \in z \ \Rightarrow \ x \in^* t) \\
z \in^* \bigcup t & \equiv & \exists y \ (y \in^* t \wedge z \in y) \\
z \in^* \{x \in t \mid \phi\} & \equiv & z \in^* t \ \wedge \ \phi^*\{x := z\}
\end{array}$$

$$\begin{array}{rcl@{\qquad\qquad}rcl}
(t = u)^* & \equiv & \forall z \ (z \in^* t \Leftrightarrow z \in^* u) & (\phi \wedge \psi)^* & \equiv & \phi^* \wedge \psi^* \\
(t \in u)^* & \equiv & \exists z \ ((z = t)^* \wedge z \in^* u) & (\phi \vee \psi)^* & \equiv & \phi^* \vee \psi^* \\
 & & & (\phi \Rightarrow \psi)^* & \equiv & \phi^* \Rightarrow \psi^* \\
\top^* & \equiv & \top & (\forall x \ \phi)^* & \equiv & \forall x \ \phi^* \\
\bot^* & \equiv & \bot & (\exists x \ \phi)^* & \equiv & \exists x \ \phi^*
\end{array}$$

FIGURE 2. Deskolemisation equations for terms and formulæ of Z^{sk}

FACT 1. — *For all terms t and formulæ ϕ of the language of* Z^{sk}, *one has* $FV(z \in^* t) = FV(t) \cup \{z\}$ *and* $FV(\phi^*) = FV(\phi)$.

PROOF. By mutual induction on the sizes of t and ϕ. $\dashv$

PROPOSITION 5 (Translation equivalence). — *For all terms t and formulæ ϕ of the language of* Z^{sk}, *one has:*

1. $\mathrm{IZ}^{\mathrm{sk}} \vdash (z \in^* t) \Leftrightarrow z \in t$
2. $\mathrm{IZ}^{\mathrm{sk}} \vdash \phi^* \Leftrightarrow \phi$

Moreover, if ϕ is expressed in the core language of set theory, then:

3. $\mathrm{IZ} \vdash \phi^* \Leftrightarrow \phi$

PROOF. Items 1. and 2. are proved by mutual induction on the sizes of t and ϕ. We distinguish cases according to the construction of t and ϕ:

- t is a variable x. Trivial, since $z \in^* x$ is $z \in x$.

- t is ω. We have to prove $(z \in^* \omega) \Leftrightarrow z \in \omega$, that is: $\mathrm{nat}(z) \Leftrightarrow z \in \omega$. This is obvious from (Infinity$^{\mathrm{sk}}$).
- t is $\{t_1; t_2\}$. We have to prove $(z \in^* \{t_1; t_2\}) \Leftrightarrow z \in \{t_1; t_2\}$, that is, $(z = t_1)^* \vee (z = t_2)^* \Leftrightarrow z \in \{t_1; t_2\}$, which is also

  $$\forall y\ (y \in z \Leftrightarrow y \in^* t_1) \vee \forall y\ (y \in z \Leftrightarrow y \in^* t_1) \Leftrightarrow z \in \{t_1; t_2\}\,.$$

  By induction hypothesis, we know that both $(y \in^* t_1) \Leftrightarrow y \in t_1$ and $(y \in^* t_2) \Leftrightarrow y \in t_2$ are provable. Hence we have to prove

  $$\forall y\ (y \in z \Leftrightarrow y \in t_1) \vee \forall y\ (y \in z \Leftrightarrow y \in t_1) \Leftrightarrow z \in \{t_1; t_2\}\,.$$

  But this is obvious from extensionality[3] and (Pairing$^{\mathrm{sk}}$).
- t is $\mathfrak{P}(t_1)$ or $\bigcup t_1$. Both cases are analogous to the latter case.
- t is $\{x \in t_1 \mid \phi_1\}$. We have to prove

  $$(z \in^* \{x \in t_1 \mid \phi_1\}) \ \Leftrightarrow\ z \in \{x \in t_1 \mid \phi_1\}\,,$$

  that is

  $$z \in^* t_1 \wedge \phi_1^*\{x := z\} \ \Leftrightarrow\ z \in \{x \in t_1 \mid \phi_1\}\,.$$

  By induction hypothesis, we know that both $(z \in^* t_1) \Leftrightarrow z \in t_1$ and $\phi_1^* \Leftrightarrow \phi_1$ are provable. Hence we have to prove

  $$z \in t_1 \wedge \phi_1\{x := z\} \ \Leftrightarrow\ z \in \{x \in t_1 \mid \phi_1\}\,.$$

  But this is obvious from (Compr.$^{\mathrm{sk}}$).
- ϕ is $t = u$. We have to prove $(t = u)^* \Leftrightarrow t = u$, that is

  $$\forall z\ (z \in^* t \Leftrightarrow z \in^* u) \ \Leftrightarrow\ t = u\,.$$

  By induction hypothesis, we know that both formulæ $(z \in^* t) \Leftrightarrow z \in t$ and $(z \in^* u) \Leftrightarrow z \in u$ are provable. Hence we have to prove

  $$\forall z\ (z \in t \Leftrightarrow z \in u) \ \Leftrightarrow\ t = u\,.$$

  But this is obvious from extensionality.
- ϕ is $t \in u$. We have to prove $\exists z\ ((z = t)^* \wedge z \in^* u) \ \Leftrightarrow\ t \in u$, that is

  $$\exists z\ (\forall y\ (y \in z \Leftrightarrow y \in^* t) \wedge z \in^* u) \ \Leftrightarrow\ t \in u\,.$$

  By induction hypothesis, we know that both formulæ $(y \in^* t) \Leftrightarrow y \in t$ and $(z \in^* u) \Leftrightarrow z \in u$ are provable. Hence we have to prove

  $$\exists z\ (\forall y\ (y \in z \Leftrightarrow y \in t) \wedge z \in u) \ \Leftrightarrow\ t \in u\,.$$

  From extensionality, the formula above is equivalent to

  $$\exists z\ (z = t \wedge z \in u) \ \Leftrightarrow\ t \in u\,,$$

  which is obvious from the equality axioms.
- ϕ is $\top$ or $\bot$. Trivial, since ϕ^* is ϕ.
- ϕ is $\phi_1 \wedge \phi_2$. We have to prove $(\phi_1 \wedge \phi_2)^* \Leftrightarrow \phi_1 \wedge \phi_2$, that is the formula $\phi_1^* \wedge \phi_2^* \Leftrightarrow \phi_1 \wedge \phi_2$. But this is obvious from the equivalences $\phi_1^* \Leftrightarrow \phi_1$ and $\phi_2^* \Leftrightarrow \phi_2$ that come from induction hypothesis.
- ϕ is $\phi_1 \vee \phi_2$ or $\phi_1 \Rightarrow \phi_2$. Both cases are analogous to the latter case.

[3]By extensionality, we mean the equivalence $\forall z\ (z \in a \Leftrightarrow z \in b) \ \Leftrightarrow\ a = b$, which follows from (Ext.) (direct implication) and (Compat-Left) (converse implication).

- ϕ is $\forall x\,\phi_1$. We have to prove $(\forall x\,\phi_1)^* \Leftrightarrow \forall x\,\phi_1$, that is: $\forall x\,\phi_1^* \Leftrightarrow \forall x\,\phi_1$. But this is obvious from the equivalence $\phi_1^* \Leftrightarrow \phi_1$ which comes from induction hypothesis.
- ϕ is $\exists x\,\phi_1$. This case is analogous to the latter case.

The last item (3.) is proved separately, by structural induction on ϕ. The only interesting cases correspond to atomic formulæ:

- ϕ is $x = y$. We have to prove $(x = y)^* \Leftrightarrow x = y$ in IZ, that is:

$$\forall z\ (z \in x \Leftrightarrow z \in y)\ \Leftrightarrow\ x = y\,.$$

  This is obvious from extensionality (expressed in IZ).
- ϕ is $x \in y$. We have to prove $(x \in y)^* \Leftrightarrow x \in y$ in IZ, that is the formula $\exists z\ ((z = x)^* \wedge z \in^* y)\ \Leftrightarrow\ x \in y$, which is also:

$$\exists z\ (\forall w\ (w \in z \Leftrightarrow w \in x)\ \wedge\ z \in y)\ \Leftrightarrow\ x \in y\,.$$

  But this is obvious from the equality axioms and extensionality (in IZ).

The rest of the proof (i.e. treating inductive cases) is then pure routine. ⊣

We now have to prove that the deskolemisation procedure transforms each theorem ϕ of (I)Z$^{\mathrm{sk}}$ into a theorem ϕ^* of (I)Z. For that, we have to check—and this is the crucial point—that each term of the extended language Z$^{\mathrm{sk}}$ corresponds to a set whose existence can be proved in IZ, that is:

Lemma 1 (Collection). — *For every term t of* Z$^{\mathrm{sk}}$*, one has:*

$$\mathrm{IZ}\ \vdash\ \exists x\ \forall z\ (z \in x \Leftrightarrow z \in^* t) \qquad\qquad (x \textit{ and } z \textit{ fresh w.r.t. } t)$$

Proof. By structural induction on the size of t, distinguishing the following cases:

- t is ω. We have to prove $\exists x\ \forall z\ (z \in x \Leftrightarrow z \in^* \omega)$ in IZ, that is the formula $\exists x\ \forall z\ (z \in x \Leftrightarrow \mathrm{nat}(z))$. But this is precisely (Infinity).
- t is $\{t_1; t_2\}$. We have to prove $\exists x\ \forall z\ (z \in x \Leftrightarrow z \in^* \{t_1; t_2\})$ in IZ, that is, $\exists x\ \forall z\ (z \in x \Leftrightarrow (z = t_1)^* \vee (z = t_2)^*)$, which is the formula:

$$\exists x\ \forall z\ (z \in x \Leftrightarrow \forall y\ (y \in z \Leftrightarrow y \in^* t_1) \vee \forall y\ (y \in z \Leftrightarrow y \in^* t_2))\,.$$

  By induction hypothesis, there are sets x_1 and x_2 such that

$$\forall y\ (y \in x_1 \Leftrightarrow y \in^* t_1) \qquad \text{and} \qquad \forall y\ (y \in x_2 \Leftrightarrow y \in^* t_2)\,.$$

  From these equivalences, the formula we have to prove is equivalent to

$$\exists x\ \forall z\ (z \in x \Leftrightarrow \forall y\ (y \in z \Leftrightarrow y \in x_1) \vee \forall y\ (y \in z \Leftrightarrow y \in x_2))\,,$$

  that is to the formula $\exists x\ \forall z\ (z \in x \Leftrightarrow z = x_1 \vee z = x_2)$ (by extensionality), which is an immediate consequence of the pairing axiom.
- t is $\mathfrak{P}(t_1)$ or $\bigcup t_1$. Both cases are analogous to the latter case.
- t is $\{y \in t_1 \mid \phi_1\}$. We have to prove $\exists x\ \forall z\ (z \in x \Leftrightarrow z \in^* \{y \in t_1 \mid \phi_1\})$ in IZ, that is the formula

$$\exists x\ \forall z\ (z \in x \Leftrightarrow z \in^* t_1 \wedge \phi_1^*\{y := z\})$$

  By induction hypothesis, there exists a set x_1 such that

$$\forall z\ (z \in x_1 \Leftrightarrow z \in^* t_1)\,,$$

so that the formula we have to prove is equivalent to

$$\exists x\ \forall z\ (z \in x \Leftrightarrow z \in x_1 \wedge \phi_1^*\{y := z\})\,,$$

which is a consequence of the comprehension scheme.

⊣

Lemma 2. — *If ϕ is an axiom of* Z^{sk}*, then* $\mathrm{IZ} \vdash \phi^*$*.*

Proof. Let ϕ be an axiom of Z^{sk}. We distinguish the following cases:

- The formula ϕ is an equality axiom, or the axiom of extensionality. In this case, ϕ is also an axiom of IZ, and since $\mathrm{IZ} \vdash \phi^* \Leftrightarrow \phi$ (Prop. 5, item 3.) we get $\mathrm{IZ} \vdash \phi^*$.
- The formula ϕ is $\forall a\ \forall b\ \forall x\ (x \in \{a;b\} \Leftrightarrow x = a \vee x = b)$ (Pairing$^{\mathrm{sk}}$). In this case, the formula ϕ^* is
$$\begin{array}{rcl} \phi^* & \equiv & \forall a\ \forall b\ \forall x\ (\exists z\ ((z = x)^* \wedge z \in^* \{a;b\}) \\ & & \qquad\qquad \Leftrightarrow (x = a)^* \vee (x = b)^*) \\ & \equiv & \forall a\ \forall b\ \forall x\ (\exists z\ ((z = x)^* \wedge ((z = a)^* \vee (z = b)^*)) \\ & & \qquad\qquad \Leftrightarrow (x = a)^* \vee (x = b)^*) \end{array}$$
But ϕ^* is a consequence of the equality axioms and (Ext.)
- The formula ϕ is either the powerset axiom (Powerset$^{\mathrm{sk}}$), the union axiom (Union$^{\mathrm{sk}}$), or the infinity axiom (Infinity$^{\mathrm{sk}}$). These cases are analogous to the latter case.
- The formula ϕ is an instance of the comprehension scheme (Compr.$^{\mathrm{sk}}$):
$$\phi \equiv \forall x_1 \cdots \forall x_n\ \forall a\ \forall y\ (y \in \{x \in a \mid \psi\} \Leftrightarrow y \in a \wedge \psi\{x := y\})$$
(for some formula ψ of Z^{sk} whose free variables occur among the variables $x_1, \ldots, x_n$ and x). Then ϕ^* is
$$\begin{array}{rcl} \phi^* & \equiv & \forall x_1 \cdots \forall x_n\ \forall a\ \forall y\ (\exists z\ (z = y \wedge z \in^* \{x \in a \mid \psi\}) \\ & & \qquad\qquad\qquad\qquad \Leftrightarrow (y \in a)^* \wedge (\psi\{x := y\})^*) \\ & \equiv & \forall x_1 \cdots \forall x_n\ \forall a\ \forall y\ (\exists z\ (z = y \wedge z \in a \wedge \psi^*\{x := z\}) \\ & & \qquad\qquad\qquad\qquad \Leftrightarrow \exists z\ (z = y \wedge z \in a) \wedge \psi^*\{x := y\}) \end{array}$$
But ϕ^* a consequence of the equality axioms and (Ext).

⊣

Remark 1. — It is interesting to notice that the proof (in IZ) of the translation ϕ^* of *every* axiom ϕ of Z^{sk} only relies on the equality axioms and the extensionality axiom of Zermelo's theory—even when ϕ is the Skolemised version of one of Zermelo's existential axioms. This paradoxical fact does not mean that Zermelo's existential axioms play no role during the translation of proofs from (I)Z^{sk} to (I)Z, but simply that this role is played somewhere else. As we shall see in the rest of this section, Zermelo's existential axioms actually come into action in the translation of the deduction rules involving a substitution, since the lemma that describes the interaction between the deskolemisation procedure and substitution relies on them:

Lemma 3 (Substitutivity). — *For all formulæ ϕ and for all terms t and u of* Z^{sk} *one has the equivalences:*

1. IZ $\vdash\ y \in^* t\{x := u\} \ \Leftrightarrow\ \exists x\ (y \in^* t\ \wedge\ \forall z\ (z \in x \Leftrightarrow z \in^* u)) \quad (y \not\equiv x)$
2. IZ $\vdash\ (\phi\{x := u\})^* \ \Leftrightarrow\ \exists x\ (\phi^*\ \wedge\ \forall z\ (z \in x \Leftrightarrow z \in^* u))$

PROOF. We first prove by mutual induction on t and ϕ that:

1. IZ $\vdash\ \forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u)\ \Rightarrow\ \forall z\ (z \in^* t\{x := u\} \Leftrightarrow z \in^* t))$
2. IZ $\vdash\ \forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u)\ \Rightarrow\ (\phi\{x := u\}^* \Leftrightarrow \phi))$

We distinguish the following cases:

- t is the variable x. We have to prove

  $$\forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u)\ \Rightarrow\ \forall z\ (z \in^* x\{x := u\} \Leftrightarrow z \in^* x))$$

  that is, the formula

  $$\forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u)\ \Rightarrow\ \forall z\ (z \in^* u \Leftrightarrow z \in x))\,,$$

  which holds by purely logical means.
- t is a variable $y \not\equiv x$. We have to prove

  $$\forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u)\ \Rightarrow\ \forall z\ (z \in^* y\{x := u\} \Leftrightarrow z \in^* y))$$

  that is, the formula

  $$\forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u)\ \Rightarrow\ \forall z\ (z \in y \Leftrightarrow z \in y))\,,$$

  which holds by purely logical means.
- t is ω. We have to prove

  $$\forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u)\ \Rightarrow\ \forall z\ (z \in^* \omega\{x := u\} \Leftrightarrow z \in^* \omega))$$

  that is, the formula

  $$\forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u)\ \Rightarrow\ \forall z\ (z \in^* \omega \Leftrightarrow z \in^* \omega))\,,$$

  which holds by purely logical means.
- t is $\{t_1; t_2\}$. Assume that x is a set such that $\forall z\ (z \in x \Leftrightarrow z \in^* u)$ $(*)$. Under this assumption, we have to prove

  $$\forall z\ (z \in^* \{t_1; t_2\}\{x := u\}\ \Leftrightarrow\ z \in^* \{t_1; t_2\})\,,$$

  that is the formula

  $$\forall z\ ((z = t_1\{x := u\})^* \vee (z = t_2\{x := u\})^*\ \Leftrightarrow\ (z = t_1)^* \vee (z = t_2)^*)\,.$$

  By induction hypothesis, we know that the equivalences

  $$\begin{array}{c}\forall y\ (y \in^* t_1\{x := u\} \Leftrightarrow y \in^* t_1)\\ \forall y\ (y \in^* t_2\{x := u\} \Leftrightarrow y \in^* t_2)\end{array}$$

  are provable under the assumption $(*)$, from which we easily deduce the equivalences

  $$\begin{array}{rcl}(z = t_1\{x := u\})^* & \Leftrightarrow & (z = t_1)^*\\ (z = t_2\{x := u\})^* & \Leftrightarrow & (z = t_2)^*\end{array}$$

  (using the definition: $(z = t)^* \equiv \forall y\ (y \in z \Leftrightarrow y \in^* t)$). The desired formula comes from the latter equivalences by purely logical means.
- t is $\mathfrak{P}(t_1)$ or $\bigcup t_1$. These cases are analogous to the latter.

- t is $\{y \in t_1 \mid \phi_1\}$. Assume that x is a set such that $\forall z\ (z \in x \Leftrightarrow z \in^* u)$ $(*)$. Under this assumption, we have to prove

  $$\forall z\ (z \in^* \{y \in t_1 \mid \phi_1\}\{x := u\} \ \Leftrightarrow\ z \in^* \{y \in t_1 \mid \phi_1\})\,,$$

  that is, the formula

  $$\forall z\ (z \in^* t_1\{x := u\} \wedge \phi_1\{x := u\}\{y := z\} \Leftrightarrow\ z \in^* t_1 \wedge \phi_1\{y := z\})\,.$$

  By induction hypothesis, we know that the equivalences

  $$\begin{array}{c}\forall y\ (y \in^* t_1\{x := u\} \ \Leftrightarrow\ y \in^* t_1) \\ \phi_1\{x := u\}^* \ \Leftrightarrow\ \phi^*\end{array}$$

  are provable under the assumption $(*)$, from which we easily deduce the equivalence

  $$\phi_1\{x := u\}\{y := z\}^* \ \Leftrightarrow\ \phi_1^*\{y := z\}$$

  (since y does not appear in the assumption $(*)$). The desired formula then comes from these equivalences by purely logical means.
- ϕ is $t_1 = t_2$. Assume that x is a set such that $\forall z\ (z \in x \Leftrightarrow z \in^* u)$ $(*)$. Under this assumption, we have to prove the equivalence

  $$(t_1 = t_2)\{x := u\}^* \ \Leftrightarrow\ (t_1 = t_2)^*\,,$$

  that is, the formula

  $$\forall z\ (z \in^* t_1\{x := u\} \Leftrightarrow z \in^* t_2\{x := u\}) \ \Leftrightarrow\ \forall z\ (z \in^* t_1 \Leftrightarrow z \in^* t_2)\,.$$

  By induction hypothesis, we know that the equivalences

  $$\begin{array}{c}\forall z\ (z \in^* t_1\{x := u\} \Leftrightarrow z \in^* t_1) \\ \forall z\ (z \in^* t_2\{x := u\} \Leftrightarrow z \in^* t_2)\end{array}$$

  are provable under the assumption $(*)$, so that the desired equivalence immediately follows by purely logical means.
- ϕ is $t_1 \in t_2$. Assume that x is a set such that $\forall z\ (z \in x \Leftrightarrow z \in^* u)$ $(*)$. Under this assumption, we have to prove the equivalence

  $$(t_1 \in t_2)\{x := u\}^* \ \Leftrightarrow\ (t_1 \in t_2)^*\,,$$

  that is, the formula

  $$\exists y\ ((y = t_1\{x := u\})^* \wedge y \in^* t_2\{x := u\}) \ \Leftrightarrow\ \exists y\ ((y = t_1)^* \wedge y \in^* t_2)\,,$$

  which is also the formula

  $$\begin{array}{l}\exists y\ (\forall z\ (z \in y \Leftrightarrow z \in^* t_1\{x := u\}) \ \wedge\ y \in^* t_2\{x := u\}) \\ \Leftrightarrow \exists y\ (\forall z\ (z \in y \Leftrightarrow z \in^* t_1) \ \wedge\ y \in^* t_2)\,,\end{array}$$

  By induction hypothesis, we know that the equivalences

  $$\begin{array}{c}\forall z\ (z \in^* t_1\{x := u\} \Leftrightarrow z \in^* t_1) \\ \forall y\ (y \in^* t_2\{x := u\} \Leftrightarrow y \in^* t_2)\end{array}$$

  are provable under the assumption $(*)$, so that the desired equivalence immediately follows by purely logical means.
- ϕ is $\top$ or $\bot$. Obvious.

- ϕ is $\phi_1 \wedge \phi_2$. Assume that x is a set such that $\forall z\ (z \in x \Leftrightarrow z \in^* u)$ $(*)$. Under this assumption, we have to prove the equivalence
$$(\phi_1 \wedge \phi_2)\{x := u\}^* \;\Leftrightarrow\; (\phi_1 \wedge \phi_2)^*\,,$$
that is, the formula
$$\phi_1\{x := u\}^* \wedge \phi_2\{x := u\}^* \Leftrightarrow\; \phi_1^* \wedge \phi_2^*\,.$$
By induction hypothesis, we know that the equivalences
$$\phi_1\{x := u\}^* \Leftrightarrow \phi_1^* \qquad \text{and} \qquad \phi_2\{x := u\}^* \Leftrightarrow \phi_2^*$$
are provable under the assumption $(*)$, so that the desired equivalence immediately follows by purely logical means.
- ϕ is $\phi_1 \vee \phi_2$ or $\phi_1 \Rightarrow \phi_2$. These cases are analogous to the latter case.
- ϕ is $\forall y\ \phi_1$. Assume that x is a set such that $\forall z\ (z \in x \Leftrightarrow z \in^* u)$ $(*)$. Under this assumption, we have to prove the equivalence
$$(\forall y\ \phi_1)\{x := u\}^* \;\Leftrightarrow\; (\forall y\ \phi_1)^*\,,$$
that is, the formula
$$\forall y\ \phi_1\{x := u\}^* \;\Leftrightarrow\; \forall y\ \phi_1^*\,.$$
By induction hypothesis, we know that the equivalence
$$\phi_1\{x := u\}^* \Leftrightarrow \phi_1^*$$
is provable under the assumption $(*)$ (which does not refer to y), so that the desired equivalence immediately follows by purely logical means.
- ϕ is $\exists y\ \phi_1$. This case is analogous to the latter case.

We established that for each term t and each formula ϕ the formulæ
$$\begin{array}{l}\forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u) \;\Rightarrow\; \forall z\ (z \in^* t\{x := u\} \Leftrightarrow z \in^* t))\\ \forall x\ (\forall z\ (z \in x \Leftrightarrow z \in^* u) \;\Rightarrow\; (\phi\{x := u\}^* \Leftrightarrow \phi))\end{array}$$
are provable in IZ, from which the equivalences
$$\begin{array}{rcl} y \in^* t\{x := u\} & \Leftrightarrow & \exists x\ (y \in^* t \;\wedge\; \forall z\ (z \in x \Leftrightarrow z \in^* u))\\ (\phi\{x := u\})^* & \Leftrightarrow & \exists x\ (\phi^* \;\wedge\; \forall z\ (z \in x \Leftrightarrow z \in^* u))\end{array}$$
immediately follow by Lemma 1. ⊣

Lemma 4 (Deskolemisation of a derivation). — *Let A be a formula and Γ a list of formulæ both expressed in the language of Z^{sk}. If the sequent $\Gamma \vdash A$ is classically (resp. intuitionistically) derivable, then there exists a list Δ of axioms of Zermelo's set theory such that the sequent $\Delta, \Gamma^* \vdash A^*$ is classically (resp. intuitionistically) derivable.*

Proof. By induction of the derivation π of $\Gamma \vdash A$. The only interesting cases correspond to the rules of inference that involve a substitution, that is, the rules $\exists$-intro and $\forall$-elim.

- ($\exists$-intro) The classical (resp. intuitionistic) derivation π has the form
$$\pi = \left\{\begin{array}{c} \vdots\ \pi_1 \\ \dfrac{\Gamma \vdash \phi\{x := t\}}{\Gamma \vdash \exists x\, \phi}\end{array}\right.$$

By induction hypothesis, there exists a context Δ_1 formed by axioms of Z and a classical (resp. intuitionistic) derivation π_1^* of the form:

$$\begin{array}{c} \vdots\ \pi_1^* \\ \Delta_1, \Gamma^* \vdash (\phi\{x := t\})^* \end{array}$$

From lemma 3, we know that

$$\mathrm{IZ}\ \vdash\ (\phi\{x := t\})^* \Leftrightarrow \exists x\ (\phi^* \wedge \forall z\ (z \in x \Leftrightarrow z \in^* t))$$

hence

$$\mathrm{IZ}\ \vdash\ (\phi\{x := t\})^* \Rightarrow \exists x\ \phi^*\,.$$

Writing Δ_1' the list of axioms which is needed to prove the latter implication, we finally build a classical (resp. intuitionistic) derivation π^* of the desired form

$$\frac{\begin{array}{c} \vdots\ \pi_1^* \\ \Delta_1, \Gamma^* \vdash (\phi\{x := t\})^* \end{array} \qquad \begin{array}{c} \vdots \\ \Delta_1' \vdash (\phi\{x := t\})^* \Rightarrow \exists x\ \phi^* \end{array}}{\Delta_1, \Delta_1', \Gamma^* \vdash (\exists x\ \phi)^*}$$

(implicitly using the admissible rule of weakening).

- ($\forall$-elim) The classical (resp. intuitionistic) derivation π has the form

$$\pi = \left\{ \frac{\begin{array}{c} \vdots\ \pi_1 \\ \Gamma \vdash \forall x\, \phi \end{array}}{\Gamma \vdash \phi\{x := t\}} \right.$$

By induction hypothesis, there exists a context Δ_1 formed by axioms of Z and a classical (resp. intuitionistic) derivation π_1^* of the form:

$$\begin{array}{c} \vdots\ \pi_1^* \\ \Delta_1, \Gamma^* \vdash \forall x\, \phi^* \end{array}$$

From lemma 3, we know that

$$\mathrm{IZ}\ \vdash\ (\phi\{x := t\})^* \Leftrightarrow \exists x\ [\phi^* \wedge \forall z\ (z \in x \Leftrightarrow z \in^* t)]\,.$$

Since by lemma 1 we have

$$\mathrm{IZ}\ \vdash\ \exists x\ (\forall z\ (z \in x \Leftrightarrow z \in^* t))\,,$$

we easily get

$$\mathrm{IZ}\ \vdash\ \forall x\ \phi^*\ \ \Rightarrow\ \ (\phi\{x := t\})^*$$

Writing Δ_1' the list of axioms which is needed to prove the latter implication, we finally build a derivation π^* of the desired form

$$\frac{\begin{array}{c} \vdots\ \pi_1^* \\ \Delta_1, \Gamma^* \vdash \forall x\, \phi^* \end{array} \qquad \begin{array}{c} \vdots \\ \Delta_1' \vdash \forall x\, \phi^* \Rightarrow (\phi\{x := t\})^* \end{array}}{\Delta_1, \Delta_1', \Gamma^* \vdash (\phi\{x := t\})^*}$$

(implicitly using the admissible rule of weakening).

The other cases are straightforward. $\dashv$

PROPOSITION 6 (Soundness of deskolemisation). — *If a closed formula ϕ is a theorem of* (I)Z^{sk}*, then ϕ^* is a theorem of* (I)Z.

PROOF. Immediately follows from lemmas 2 and 4. ⊣

PROPOSITION 7 (Conservativity). — *The theory* (I)Z$^{\mathrm{sk}}$ *is a conservative extension of* (I)Z.

PROOF. Assume that ϕ is a theorem of (I)Z$^{\mathrm{sk}}$ expressed in the language of set theory. By Prop. 6, ϕ^* is a theorem of (I)Z. But since IZ $\vdash \phi^* \Leftrightarrow \phi$ (Prop. 5, item 3.) the formula ϕ is a theorem of (I)Z. ⊣

§4. Definable constructions.

4.1. Some abbreviations. Most standard mathematical notations can be recovered in Z$^{\mathrm{sk}}$ as macros:

- Basic operations on sets:

$$\begin{array}{rcl} x \cup y & = & \bigcup\{x; y\} \\ x \cap y & = & \{z \in x \mid z \in y\} \\ x \setminus y & = & \{z \in x \mid z \notin y\} \end{array} \qquad \begin{array}{rcl} \varnothing & = & \{x \in \omega \mid \bot\} \\ \{x\} & = & \{x; x\} \end{array}$$

- Natural numbers (using von Neumann encoding):

$$0 \ = \ \varnothing \qquad\qquad s(x) \ = \ x \cup \{x\}$$

  So that we can set: $1 = s(0)$, $2 = s(1)$, $3 = s(2)$, $4 = s(3)$, etc.

- Ordered pairs and projections:

$$\begin{array}{rcl} \langle x; y\rangle & = & \{\{x\}; \{x; y\}\} \\ \pi_1(c) & = & \bigcup\{x \in \bigcup c \mid \exists y\ (c = \langle x; y\rangle)\} \\ \pi_2(c) & = & \bigcup\{y \in \bigcup c \mid \exists x\ (c = \langle x; y\rangle)\} \end{array}$$

- Cartesian product and disjoint union:

$$\begin{array}{rcl} A \times B & = & \big\{c \in \mathfrak{P}(\mathfrak{P}(A \cup B)) \mid \exists x\, \exists y\ (c = \langle x; y\rangle)\big\} \\ A + B & = & (\{0\} \times A) \cup (\{1\} \times B) \end{array}$$

In set theory, a function is represented as a set of pairs f such that the binary relation $\langle x; y\rangle \in f$ is functional w.r.t. x, that is:

$$\begin{array}{rcl} \mathrm{function}(f) & = & \forall c \in f\ \exists x\ \exists y\ (c = \langle x; y\rangle)\ \wedge \\ & & \forall x\ \forall y\ \forall y'\ (\langle x; y\rangle \in f \wedge \langle x; y'\rangle \in f \Rightarrow y = y') \end{array}$$

From this we can define the following notations:

- Domain and image of a function:

$$\begin{array}{rcl} \mathrm{dom}(f) & = & \big\{x \in \bigcup\bigcup f\ \big|\ \exists y\ (\langle x; y\rangle \in f)\big\} \\ \mathrm{img}(f) & = & \big\{y \in \bigcup\bigcup f\ \big|\ \exists x\ (\langle x; y\rangle \in f)\big\} \end{array}$$

- Function application:

$$f(x) \ = \ \bigcup\big\{y \in \bigcup\bigcup f \mid \langle x; y\rangle \in f\big\}$$

- Function space (i.e. set-theoretic exponential):

$$B^A \ = \ \big\{f \in \mathfrak{P}(A \times B) \mid \mathrm{function}(f) \wedge \mathrm{dom}(f) = A \wedge \mathrm{img}(f) \subseteq B\big\}$$

4.2. A weak form of replacement. Zermelo and Fraenkel's set theory extends Zermelo's with an additional axiom scheme, namely, Fraenkel and Skolem's *replacement scheme*

$$\text{(Repl.)} \qquad \forall a\ \big(\forall x \in a\ \exists! y \in b\ \phi(x,y)\ \Rightarrow\ \exists b\ \forall x \in a\ \exists y \in b\ \phi(x,y)\big)$$

expressing that given a set a and a binary relation $\phi(x,y)$ that is functional w.r.t. x (for $x \in a$), we can build the image of a through the relation ϕ, that is, the set b formed by all the objects y such that $\phi(x,y)$ for some $x \in a$.

In this subsection we aim to show that the weak form of replacement we obtain by only considering functional relations of the form '$y = t(x)$' where $t(x)$[4] is a term written in the language of Z^{sk} already holds in Z^{sk}, and that we can actually define the notation $\{t(x) \mid x \in u\}$ in the term language of Z^{sk}.

For that, we first define a notation $\mathsf{B}\,(t \mid x \in u)$ which intuitively represents an upper bound of the set we want to define, that is, a set which contains—at least—all the objects of the form $t(x)$ when x ranges over u.

Formally, the notation $\mathsf{B}\,(t \mid x \in u)$ is defined by induction on t as follows:

$$\begin{array}{lcl}
\mathsf{B}\,(x \mid x \in u) & = & u \\
\mathsf{B}\,(y \mid x \in u) & = & \mathfrak{P}(y) \qquad (\text{if } y \not\equiv x) \\
\mathsf{B}\,(\omega \mid x \in u) & = & \mathfrak{P}(\omega) \\
\mathsf{B}\,(\{t_1; t_2\} \mid x \in u) & = & \mathfrak{P}\big(\mathsf{B}\,(t_1 \mid x \in u) \cup \mathsf{B}\,(t_2 \mid x \in u)\big) \\
\mathsf{B}\,(\mathfrak{P}(t) \mid x \in u) & = & \mathfrak{P}(\mathfrak{P}(\bigcup \mathsf{B}\,(t \mid x \in u))) \\
\mathsf{B}\,(\bigcup t \mid x \in u) & = & \mathfrak{P}(\bigcup\bigcup \mathsf{B}\,(t \mid x \in u)) \\
\mathsf{B}\,(\{y \in t \mid \phi\} \mid x \in u) & = & \mathfrak{P}(\bigcup \mathsf{B}\,(t \mid x \in u))
\end{array}$$

The notation $\mathsf{B}\,(t \mid x \in u)$ has the expected behavior w.r.t. variable binding: it binds all the free occurrences of the variable x in the term t while keeping free all the free occurrences of x in u (that refer to the enclosing context):

Fact 2. — *For all terms t and u of Z^{sk}, one has:*

$$FV\big(\mathsf{B}\,(t \mid x \in u)\big)\ \subseteq\ (FV(t) \setminus \{x\}) \cup FV(u)\,.$$

We have to prove that the term $\mathsf{B}\,(t \mid x \in u)$ fulfils the desired invariant:

Lemma 5. — *For all terms $t(x)$ and u of Z^{sk} such that $x \notin FV(u)$:*

$$\mathrm{IZ}^{\mathrm{sk}}\ \vdash\ \forall x\ (x \in u \Rightarrow t(x) \in \mathsf{B}\,(t(x) \mid x \in u))\,.$$

Proof. By induction on the term $t(x)$.

- $t(x)$ is the variable x. We have to prove $\forall x\ (x \in u \Rightarrow x \in \mathsf{B}\,(x \mid x \in u))$, that is the formula $\forall x\ (x \in u \Rightarrow x \in u)$. Trivial.
- $t(x)$ is a variable $y \not\equiv x$. We have to prove $\forall x\ (x \in u \Rightarrow y \in \mathsf{B}\,(y \mid x \in u))$, that is the formula $\forall x\ (x \in u \Rightarrow y \in \mathfrak{P}(y))$. This is obvious.
- $t(x)$ is ω. We have to prove $\forall x\ (x \in u \Rightarrow \omega \in \mathsf{B}\,(\omega \mid x \in u))$, that is the formula $\forall x\ (x \in u \Rightarrow \omega \in \mathfrak{P}(\omega))$. This is obvious.
- $t(x)$ is $\{t_1(x); t_2(x)\}$. We have to prove

$$\forall x\ \big(x \in u\ \Rightarrow\ \{t_1(x); t_2(x)\} \in \mathsf{B}\,(\{t_1(x); t_2(x)\} \mid x \in u)\big)\,,$$

[4]Here we write $t(x)$ instead of t to emphasize that t possibly depends on x—but not on y.

that is the formula

$$\forall x\ \big(x \in u\ \Rightarrow\ \{t_1(x); t_2(x)\} \in \mathfrak{P}\big(\mathsf{B}\,(t_1(x) \mid x \in u) \cup \mathsf{B}\,(t_2(x) \mid x \in u)\big)\big)\,.$$

Assume $x \in u$. By induction hypothesis, we know that

$$t_1(x)\ \in\ \mathsf{B}\,(t_1(x) \mid x \in u) \qquad \text{and} \qquad t_2(x)\ \in\ \mathsf{B}\,(t_2(x) \mid x \in u)\ .$$

Hence we have

$$\{t_1(x); t_2(x)\}\ \subseteq\ \mathsf{B}\,(t_1(x) \mid x \in u) \cup \mathsf{B}\,(t_2(x) \mid x \in u)$$

and finally

$$\{t_1(x); t_2(x)\}\ \in\ \mathfrak{P}\big(\mathsf{B}\,(t_1(x) \mid x \in u) \cup \mathsf{B}\,(t_2(x) \mid x \in u)\big)\,.$$

- $t(x)$ is $\mathfrak{P}(t_1(x))$. We have to prove

$$\forall x\ \big(x \in u\ \Rightarrow\ \mathfrak{P}(t_1(x))\ \in\ \mathsf{B}\,(\mathfrak{P}(t_1(x)) \mid x \in u)\big)\,,$$

that is the formula

$$\forall x\ \Big(x \in u\ \Rightarrow\ \mathfrak{P}(t_1(x))\ \in\ \mathfrak{P}\Big(\mathfrak{P}\Big(\bigcup \mathsf{B}\,(t_1(x) \mid x \in u)\Big)\Big)\Big)\,.$$

Assume $x \in u$. By induction hypothesis, we get $t_1(x) \in \mathsf{B}\,(t_1(x) \mid x \in u)$. We thus have

$$t_1(x)\ \subseteq\ \bigcup \mathsf{B}\,(t_1(x) \mid x \in u)\ ,$$

hence

$$\mathfrak{P}(t_1(x))\ \subseteq\ \mathfrak{P}\Big(\bigcup \mathsf{B}\,(t_1(x) \mid x \in u)\Big)\,,$$

and finally

$$\mathfrak{P}(t_1(x))\ \in\ \mathfrak{P}\Big(\mathfrak{P}\Big(\bigcup \mathsf{B}\,(t_1(x) \mid x \in u)\Big)\Big)\,.$$

- $t(x)$ is $\bigcup t_1(x)$. We have to prove

$$\forall x\ \Big(x \in u\ \Rightarrow\ \bigcup t_1(x)\ \in\ \mathsf{B}\Big(\bigcup t_1(x) \mid x \in u\Big)\Big)\,,$$

that is the formula

$$\forall x\ \Big(x \in u\ \Rightarrow\ \bigcup t_1(x)\ \in\ \mathfrak{P}\Big(\bigcup\bigcup \mathsf{B}\,(t_1(x) \mid x \in u)\Big)\Big)\,.$$

Assume $x \in u$. By induction hypothesis, we get $t_1(x) \in \mathsf{B}\,(t_1(x) \mid x \in u)$. We thus have

$$t_1(x)\ \subseteq\ \bigcup \mathsf{B}\,(t_1(x) \mid x \in u)\ ,$$

hence

$$\bigcup t_1(x)\ \subseteq\ \bigcup\bigcup \mathsf{B}\,(t_1(x) \mid x \in u)\ ,$$

and finally

$$\bigcup t_1(x)\ \in\ \mathfrak{P}\Big(\bigcup\bigcup \mathsf{B}\,(t_1(x) \mid x \in u)\Big)\,.$$

- $t(x)$ is $\{y \in t_1(x) \mid \phi_1(x,y)\}$. We have to prove

$$\forall x\ \big(x \in u\ \Rightarrow\ \{y \in t_1(x) \mid \phi_1(x,y)\}\ \in\ \mathsf{B}\left(\{y \in t_1(x) \mid \phi_1(x,y)\} \mid x \in u\right)\big)\,,$$

that is the formula

$$\forall x\ \Big(x \in u\ \Rightarrow\ \{y \in t_1(x) \mid \phi_1(x,y)\}\ \in\ \mathfrak{P}\Big(\bigcup \mathsf{B}\left(t_1(x) \mid x \in u\right)\Big)\Big)\,.$$

Assume $x \in u$. By induction hypothesis, we get $t_1(x) \in \mathsf{B}\left(t_1(x) \mid x \in u\right)$. We thus have

$$\{y \in t_1(x) \mid \phi_1(x,y)\}\ \subseteq\ t_1(x)\ \subseteq\ \bigcup \mathsf{B}\left(t_1(x) \mid x \in u\right)\,,$$

hence

$$\{y \in t_1(x) \mid \phi_1(x,y)\}\ \in\ \mathfrak{P}\Big(\bigcup \mathsf{B}\left(t_1(x) \mid x \in u\right)\Big)\,. \qquad \dashv$$

From the lemma above we can set for all terms t and u

$$\{t \mid x \in u\}\ \equiv\ \{y \in \mathsf{B}\left(t \mid x \in u\right) \mid \exists x \in u\ (y = t)\}$$

and we easily check that

PROPOSITION 8. — *For all terms t, u such that $x \notin FV(u)$ and $y \notin FV(t)$:*

$$\mathrm{IZ}^{\mathrm{sk}}\ \vdash\ \forall y\ (y \in \{t \mid x \in u\}\ \Leftrightarrow\ \exists x\ (x \in u \land y = t))\,.$$

PROOF. Follows from lemma 5 by comprehension. $\dashv$

4.3. More abbreviations. From the notation $\{t(x) \mid x \in u\}$ we can now derive the following abbreviations:

$$\begin{array}{rcl}
\lambda x \in A\,.\,t(x) & = & \{\langle x; t(x)\rangle \mid x \in A\} \\
\displaystyle\bigcup_{x\in A} B(x) & = & \bigcup\{B(x) \mid x \in A\} \\
\displaystyle\sum_{x\in A} B(x) & = & \displaystyle\bigcup_{x\in A} \{x\} \times B(x) \\
\displaystyle\prod_{x\in A} B(x) & = & \left\{f \in \Big(\displaystyle\bigcup_{x\in A} B(x)\Big)^A\ \middle|\ \forall x \in A\ f(x) \in B(x)\right\}
\end{array}$$

4.4. Incompleteness w.r.t. Skolemisation. From the derivability of the weak form of replacement discussed in 4.2 it is possible to show that the syntactic constructs provided in Z^{sk} are actually not sufficient to express all Skolem symbols, in the sense that we can define a binary predicate $\phi(x,y)$ such that $\mathrm{Z}^{\mathrm{sk}} \vdash \forall x\, \exists y\, \phi(x,y)$ while there is no term $t(x)$ depending on x (in the language of Z^{sk}) such that $\mathrm{Z}^{\mathrm{sk}} \vdash \forall x\ \phi(x, t(x))$. An example is the following:

Let $\phi(x,y)$ be a predicate expressing that 'x is a natural number and y is the xth powerset of ω'. A possible definition of $\phi(x,y)$ is the following:

$$\begin{array}{rl}
\phi(x,y)\ \equiv\ \exists f\ \Big(& f \text{ function } \land\ \mathrm{dom}(f) = s(x)\ \land\ \mathrm{nat}(x)\ \land \\
& f(0) = \omega\ \land\ \forall z \in x\ f(s(z)) = \mathfrak{P}(f(z))\ \land\ f(x) = y\Big)
\end{array}$$

We then check that:

PROPOSITION 9. — *If Z^{sk} is consistent, then:*

1. $\mathrm{Z}^{\mathrm{sk}} \vdash \forall x \in \omega\ \exists! y\ \phi(x,y)$;
2. *There is no term $t(x)$ in Z^{sk} such that* $\mathrm{Z}^{\mathrm{sk}} \vdash \forall x \in \omega\ \phi(x, t(x))$

PROOF. 1. By induction on $x \in \omega$ (independently from the consistency of Z).

2. If there is a term $t(x)$ such that $\forall x \in \omega\ \phi(x, t(x))$, then we can form the set $a = \{t(x) \mid x \in \omega\}$ (Prop. 8) and prove that a contains ω (as an element) and is closed under the powerset operation. But it is well-known [2] that the existence of such a set cannot be proved in Zermelo's set theory unless it is inconsistent. ⊣

REFERENCES

[1] G. DOWEK., *Lambda-calculus, combinators and the comprehension scheme.*, ***Typed lambda calculi and applications***, LNCS, vol. 902, Springer-Verlag, 1995, pp. 154–170.

[2] J.-L. KRIVINE, ***Introduction to axiomatic set theory***, Springer, 1971.

[3] E. MENDELSON, ***Introduction to mathematical logic***, 4th ed., Chapman & Hall/CRC, 1997.

[4] J. R. SHOENFIELD, ***Mathematical logic***, AK Peters, 2001.

[5] A. S. TROELSTRA and H. SCHWICHTENBERG, ***Basic proof theory***, 2nd ed., Cambridge University Press, 2000.

LABORATOIRE PPS // UNIVERSITÉ PARIS DIDEROT – PARIS 7 // CASE 7014 // 75205 PARIS CEDEX 13 // FRANCE

E-mail: Alexandre.Miquel@pps.jussieu.fr